

Improved Direct Counterfactual Quantum Communication

Sheng Zhang*

Department of Electronic Technology, China Maritime Police Academy, Ningbo 315801, China

Bo Zhang and Xing-tong Liu

School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China

(Dated: May 6, 2015)

Recently, a novel direct counterfactual quantum communication protocol was proposed using chained quantum Zeno effect. We found that this protocol is far from being widely used in practical channels, due to the side effect of "chained", which leads to a dramatic increase of the equivalent optical distance between Alice and Bob. Therefore, not only the transmission time of a single bit increases in multiple times, but also the protocol is more sensitive to the noise. Here, we proposed an improved protocol, in which quantum interference is employed to destroy the nested structure induced by "chained" effect. Moreover, we proved that a better counterfactuality is easier to be achieved, and showed that our protocol outperforms the former in the presence of noises.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum communication is now widely accepted to be one of the most promising candidates in future quantum technology. Using quantum mechanics, several amazing tasks, such as dense coding[1, 2], teleportation[3, 4] and counterfactual quantum key distribution[5, 6], are naturally achieved. Since the invention of quantum key distribution(QKD) protocol, i.e., BB84 protocol[7], quantum communication has enjoyed a great success with both theoretical and commercial aspects. One of the most significant contributions, which is impossible to be achieved by classical means, is counterfactual quantum communication. It enables two remote parties, Alice and Bob, to exchange messages without transmitting any information carriers.

The idea of counterfactual quantum communication was initialized by interaction-free measurement[8–10], impressive with the phenomenon that an object can be detected without being intuitively measured. The first example, presented by Noh[5], was realized in a QKD protocol. Later, we announced a variant adapted to deterministic key distribution scenario[11]. In sharp contrast to conventional QKD schemes, these protocols are counterintuitive that the quantum states, served as the information carriers, never travel through the channel. A translated no-cloning theorem prevents the eavesdroppers from getting any information of the private key. A strict security proof of Noh's protocol(Noh09 protocol) was presented by Yin et al.[12]. We further proved that, although this protocol is secure under a general intercept-resend attack in an ideal mode, the practical security could be compromised due to the dark count rate and low efficiency of the detectors[13]. Surprisingly, we also found that Eve could get full information of the key from a real implementation by launching a counterintuitive trojan horse attack[14]. Since the rate of information photons in Noh09 protocol, only up to 12.5% in ideal setting, is not satisfactory, Sun and Wen im-

proved it to reach 50% using an iterative module[6]. Experimental verifications of Noh09 protocol have been made by various authors[15, 16].

Most interestingly, the topic of counterfactual quantum communication, has been repainted by Salih et al., who claimed a new protocol(SLAZ2013 protocol) with a better rate, using quantum Zeno effect[17]. They also announced a tripartite counterfactual quantum key distribution protocol[18], to improve the counterfactuality and security of a preview scheme by Akshata Shenoy H. et al.[19]. Other interesting applications, such as semi-counterfactual quantum cryptography[20], counterfactual quantum-information transfer[21], are also found in recent papers.

Here, we argue that it is problematic to apply SLAZ2013 protocol in real channels, unless the side effect of chained quantum Zeno effect is degraded to an acceptable level. Notice that the equivalent optical distance between Alice and Bob, being amplified by $M * N$ (numbers of the outer and inner cycles) times, is far larger than the original one, though it is good to use chained quantum Zeno effect to achieve perfect counterfactuality. Consequently, the efficiency, on the first hand, turns out to be very low. In other words, the time taken by transferring a single bit might be much longer than one expects, even though Alice and Bob stand close to each other. On the second hand, the protocol turns out to be more sensitive to the noisy, due to the increase of the equivalent distance. In [17], it was estimated that an acceptable noise rate only reaches 0.2%.

In this paper, we present a new quantum counterfactual communication protocol. The rest of the paper is organized as follow: In sectionII, our protocol is introduced. Then, we analyze the counterfactuality of both our protocol and SLAZ2013 in the following section, and it is showed that our protocol outperforms SLAZ2013 with respect to the counterfactuality and the tolerance of noise. In sectionIV, we have a brief discussion on how to bridge the presented protocol and quantum key distribution. At last, a conclusion is drawn.

*shengzhcn@gmail.com

II. PROTOCOL

First, we give a brief introduction of SLAZ2013 protocol. To achieve the goal of counterfactuality, chained quantum Zeno effect, acting as the core principle, is introduced by employing a series of beam splitters and mirrors. Correspondingly, the optical circuit is divided into two types of cycles, i.e., the outer cycle and inner cycle shown in [17]. At very beginning, a photon, which has nothing to do with the information bit, is injected by the source, and entering the input port of the outer cycle. The rest thing Alice has to do is to observe which of her detectors, D_1 and D_2 , clicks. At Bob's end, he just chooses to block(pass) the photon, if logic "1"("0") is selected to be transmitted. Let's see how Alice knows the transmitted bit. When "0" is selected, two events, denoted by E_1 and E_2 can be observed by Alice:

- (E_1) The photon has been caught in detector D_1 .
- (E_2) The photon has been caught in detector D_3 .

Note that E_2 implies that the photon has been traveling through the channel. Therefore, E_2 should be discarded. Similarly, when "1" is selected, events E_3 and E_4 can be observed:

- (E_3) The photon has been caught in detector D_2 .
- (E_4) The photon has been caught in detector D_4 .

Again, E_4 , which goes against the counterfactuality, is discarded. The central problem is that the twisted structure (i.e., outer cycle twisting with inner cycles) directly increases the optical length of the channel.

Now, we introduce our protocol. First, Let's see the setup shown in Fig.1. Compared with SLAZ2013, the only difference is easily found. We put an iterative module (shown in the dashed rectangle), which is as the same as the one in Ref.[6] or [14] except for the mirrors, to replace the inner cycle. Note that the length of each optical delay (OD) in this module should be carefully chosen to match each other. Specifically, the following condition should be satisfied,

$$L_{OD_{i+1}} - L_{OD_i} = L_0, \quad (1)$$

for $i = 1, 2, \dots, N-1$. Here, L_{OD_i} and L_0 denote the optical lengths of OD_i , and the interval between two neighbouring ODs. Also, L_{OD_1} is initialized by the optical length of the real channel in terms of matching.

Next, Let's see how this protocol works. Not surprisingly, the protocol begins with a vertically polarized photon, i.e., the state $|V\rangle$, which will be caught in detector D_1 or D_2 , according to Bob's choice 1 or 0, respectively. The explanation is presented as follow.

In Fig.2, When Bob passes the photon (all SWs are on), path i ($i = 1, 2, \dots, N$) corresponds to the optical path $PBS_1 \rightarrow MR_j$ ($j = 1, 2, \dots, N$) or $PBS_1 \rightarrow MR_B$. In this case, our protocol degrades to the first step of SLAZ2013, owing to the interference. Therefore, detector D_2 clicks with certainty. However, when all SWs are off, the interference is destroyed. Consequently, the photon will be caught in the corresponding

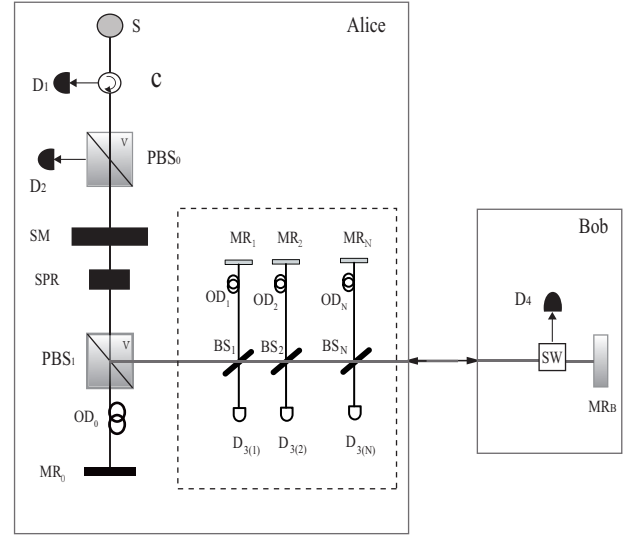


FIG. 1: Experimental setup. In contrast with SLAZ2013 protocol, an iterative module in the dashed box is introduced to replace the original inner cycle. Here, BS_i stands for a beam splitter, and $D_{3(i)}$ denotes a photon detector for $i = 1, 2, \dots, N$. Bob uses a switch (SW) to carry out the blocking operation.

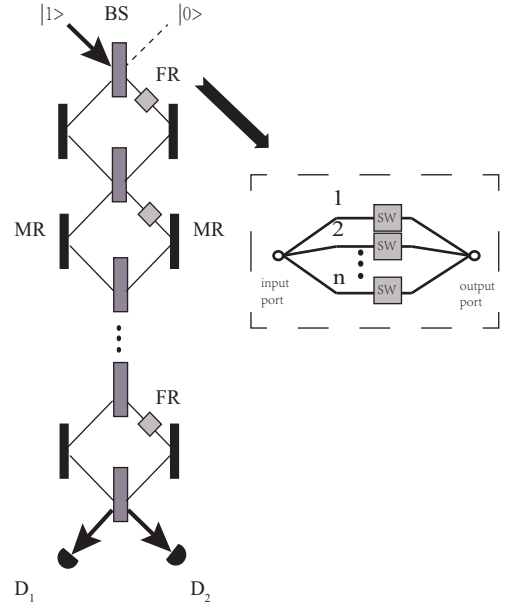


FIG. 2: Principal schematics. Here FR stands for a fictitious router, explicitly showed in the right side dashed box. The input node routes the photon to the output through one of the n paths.

detector, i.e., D_4 or $D_{3(i)}$, if it is in the right arm of the BS. In this case, our protocol is also equivalent to the first step of SLAZ2013, excepted that in which detector the photon arrives. In other words, our protocol shares the same principle with SLAZ2013 in spite of some details.

III. PERFORMANCE

In this section, we will focus our attentions on computing the counterfactuality of the presented protocol, and show that it can be achieved with less resources, in contrast with SLAZ2013 protocol. Moreover, using numerical estimating, we find that our protocol outperforms the former in the presence of channels noises.

Notice that the presented scheme is more efficient than SLAZ2013 protocol with respect to the followings: the equivalent optical distance between Alice and Bob, D_{eq} , is only $M * L$, where L denotes the practical distance. Unfortunately, we have $D_{eq} = M * N * L$ for SLAZ2013. Fortunately, the transmission time, i.e., $t = D_{eq}/C$, has been reduced by a factor of N .

A. Counterfactuality Analysis

Next, Let's see how our protocol benefits from the iterative module with respect to counterfactuality. Before the analysis begins, the conception "counterfactuality rate", denoted by C , should be reviewed. Here, it is defined by the probability of a successful communication featured with no transmission of signal carriers. Correspondingly, another conception "abnormality rate" denoted by A is defined by the reverse, so we have $A = 1 - C$. Now, we are able to define the counterfactuality of a given protocol by a pair of counterfactuality rates(or abnormality rates), $\vec{C} = (C_0, C_1)$, each representing the counterfactuality rate for Alice sending signal 0 and 1, respectively. Evidently, $C_i (i = 0, 1)$ varies from 0 to 1, and perfect counterfactual communication is available if and only if $C_i = 1 (i = 0, 1)$.

Back to SLAZ2013 protocol, it is easy to find that her counterfactuality, denoted by \vec{C}_1 , is given by P_1 and P_2 , so we have

$$\vec{C}_1 = (P_1, P_2). \quad (2)$$

Here, P_1 and P_2 are given by $P_1 = |x_M|^2$ and $P_2 = |y_{M,0}|^2$, respectively(Refer to [17] for details). This protocol achieves perfect counterfactuality when N and M approach infinity, leading to $\vec{C}_1 \rightarrow (1, 1)$, i.e., $P_1 = 1$ and $P_2 = 1$. Also note that this protocol is realized in two steps, with the following concerning: In the first step, the prototype, referring to Fig.2(a) of Ref.[17], is only partially counterfactual. In this case, the counterfactuality rate C_0 turns to be 0 for whatever N s. The second step, in which an inner cycle is employed, is introduced to improve the prototype. Therefore, the final protocol makes itself completely sound for counterfactuality. However, in our scheme, we have achieved the same goal by replacing the inner cycle with an iterative module.

Now, we begin to calculate the counterfactuality of our protocol, denoted by \vec{C}_2 , where $\vec{C}_2 = (C_0, C_1)$. When Bob blocks the channel, it is showed in Fig.2 that our protocol is an equivalent transformation of the first step of SLAZ2013. Therefore, the corresponding rate C_1 is directly deduced by quan-

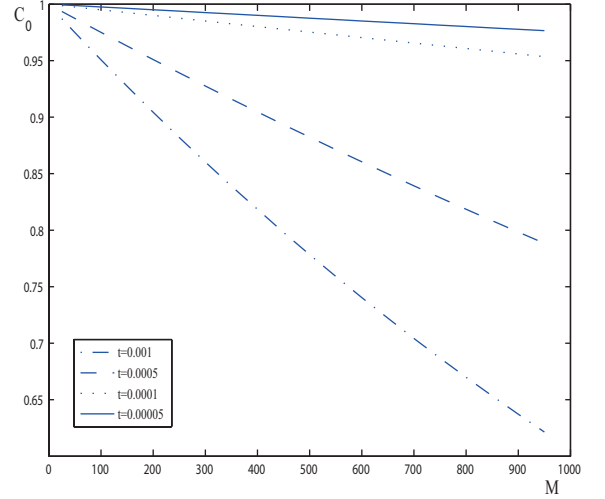


FIG. 3: C_0 as a function of M .

tum Zeno effect, i.e.,

$$C_1 = \cos^{2M} \theta, \quad (3)$$

equalling to the probability that D_1 clicks, denoted by $\text{Prob}\{D_1 \text{ clicks}\}$. Similarly, we have $\theta = \pi/2M$. Obviously, perfect counterfactuality is achievable for signal "1", when M approaches infinity.

When Bob passes the photon, i.e., signal 0 is selected, a successful counterfactual communication is established only when there is no photon in the channel for each cycle. Back to Fig.2, the probability that the photon travels through the channel in the m_{th} cycle is given by $t = \prod_{j=1}^N t_j$, where t_j is the transmissivity of the j_{th} BS inside the module. Therefore, C_0 can be written as

$$C_0 = \prod_{m=1}^M (1 - \sin^2 m\theta \cdot t). \quad (4)$$

Obviously, Eqs.(3) and (4) imply that perfect direct counterfactual communication is seen when M approaches infinity. Interestingly, one obtains $C_0 = 0$ given that $t = 1$, implying that our protocol evolves to the first step of SLAZ2013 protocol as we expected.

From above analysis, it is known that parameters N and M are crucial to achieve a better performance. We have loosely plotted the counterfactuality rate C_0 , illustrating how it varies as a function of M . In Fig.3, it is showed that all curves descend as M increases. In other words, the performance of our protocol becomes worse with a bigger M , since the probability that photon exposes itself in the channel evidently increases when the number of the cycles grows up. Fortunately, C_0 can be improved by reducing t (or independently increasing N). As is shown in Fig.3, a curve, marked with a smaller t , locates itself over the others with bigger ones. This shows that high counterfactuality (e.g., $C_0 > 0.9$) is achievable with acceptable M s, as long as t is chosen to be sufficiently small.

TABLE I: Numerical estimating results

		$M = 25$	$M = 50$	$M = 75$	$M = 100$	$M = 150$
(I) ¹	$t = 0.001$	0.987	0.975	0.963	0.951	0.927
	$t = 0.0005$	0.994	0.987	0.981	0.975	0.963
	$t = 0.0001$	0.999	0.997	0.996	0.995	0.992
	$t = 0.00005$	0.999	0.999	0.998	0.997	0.996
(II) ²	$N = 320$	0.912	0.831	0.758	0.693	0.582
	$N = 500$	0.943	0.887	0.836	0.788	0.702
	$N = 1250$	0.977	0.953	0.930	0.908	0.865
	$N = 2500$	0.988	0.976	0.964	0.953	0.930

¹ (I): The first half of the table, corresponding to our protocol. The content units are filled with values of C_0 , referring to different t s and M s.

² (II): The second half of the table, corresponding to SLAZ2013 protocol. The content units are filled with values of p_2 , referring to different M s and N s.

In order to show our advantages over SLAZ2013 protocol, we list some meaningful results, obtained from numerical estimating, in table 1. It is clear that, for SLAZ2013 protocol, N should be sufficiently large (meanwhile things getting worse as M increases), in order to achieve acceptable counterfactuality rates (bigger than 0.9). However, the same goal can be achieved, for our protocol, only by choosing an appropriate t , keeping M unchanged.

Since our protocol shares the same template with the simplified SLAZ2013 protocol, i.e, the first-step protocol, it is easy to conclude the detector rates, $Prob\{D_1 \text{ clicks}\}$ and $Prob\{D_2 \text{ clicks}\}$, which are given by $Prob\{D_1 \text{ clicks}\} = 1$ and $Prob\{D_2 \text{ clicks}\} = \cos^{2M} \theta$.

B. Robustness against Channel Noises

Here, the robustness of the presented protocol is only investigated in a most representative scenario that the channel noise acts as an obstacle which definitely registers an event of "Block". Errors only occur in case of Bob choosing to pass the photon, where interference is destroyed by noises. Remarkably, for our protocol, the presence of noises definitely induces errors as well as an increase of the probability that detector $D_{3(j)}$, ($j = 1, 2, \dots, N$) clicks, which independently discounts the performance of the protocol.

When Bob passes the photon, it will produce a click of detector D_2 with certainty owing to quantum interference, if the channel is noiseless. Let's see what happens when a "block" in one cycle is triggered by the noise other than Bob. With out loss of generality, we assume that the channel of the i_{th} cycle is blocked due to the noise. Given that the state of the i_{th} cycle is $|\varphi\rangle_{i-1} = x_i|10\rangle + y_i|01\rangle$, the quantum state after the $(i+1)_{th}$ BS is written as

$$|\varphi\rangle_{i+1} = (x_i \cos \theta - c * y_i \sin \theta)|10\rangle + (x_i \sin \theta + c * y_i \cos \theta)|01\rangle, \quad (5)$$

where c denotes the rate that the single-photon pulse in the channel of the i_{th} cycle is not absorbed. For instance, in SLAZ2013 protocol, $c = 0(1)$, corresponding to Bob's choice "Block(pass)", means that the pulse is fully(never) absorbed by Bob's detector D_4 . Interestingly, c varies from 0 to 1 for the

presented protocol, since the iterative module also contributes to the benefit that the photon in the right-hand side arm is not absorbed.

Next, it is necessary to fix the rate " c " with given parameters of the module. Suppose that a photon is reflected by PBS_1 in the i_{th} cycle, it is easy to conclude the probability that it is reflected back to PBS_1 by one of the mirrors in the module as

$$P_{ref} = \sum_{i=0}^N \prod_{j=-1}^{i-1} t_j^2 (1 - t_i)^2, \quad (6)$$

due to the absence of quantum interference. Also, the probability that it is absorbed is

$$P_{abs} = 1 - \sum_{i=0}^N \prod_{j=-1}^{i-1} t_j^2 (1 - t_i)^2 - \prod_{i=0}^N t_i. \quad (7)$$

Obviously, we have $c = P_{ref}$. Moreover, it is seen that a photon will be detected by $D_{3(j)}$, ($j = 1, 2, \dots, N$) with unit probability, when N approaches infinity [14]. Nevertheless, it is still interesting to investigate the robustness of the presented protocol in finite settings, where c is indeed a non-zero real number less than 1. In order to find how c discounts the rate of detector D_2 , we try to correlate $Prob\{D_2 \text{ clicks}\}$ with c formally. Assume independently that a single-photon pulse, denoted by an unnormalized quantum state $|\psi\rangle = c|01\rangle$, arrives at the $(i+1)_{th}$ BS in Fig.2, the final state after the following $M-i$ BSs is written by

$$|\psi\rangle_{final} = c * (\cos(M-i)\theta|01\rangle - \sin(M-i)\theta|10\rangle), \quad (8)$$

owing to quantum interference. Obviously, it is seen from Eq.8 that this independent pulse definitely contributes to the rate of detector D_2 . Therefore, $Prob\{D_2 \text{ clicks}\}$, which is given by $Prob\{D_2 \text{ clicks}\} = (1 - (1-c)y_i \cos(M-i)\theta)^2$, directly increases as c increases. Eq.6 shows the balance of c and N , and that $c = 0$ when $N \rightarrow \infty$ for the worse case. Now, we use the same technique, that random numbers between 0 and 1 are employed to play the role of noise, to plot the successful rate of the right detector. The curves in Fig.4 (a) are statistically averaged on 2000-times repetition to achieve better smoothness. Obviously, our protocol outperforms SLAZ2013 protocol on the tolerance of noise given the same M . Moreover, a smaller M implies a bigger tolerance of B for our protocol, which is consistent with the fact that an increase of the number of cycles immediately increases the risk of suffering from channel noises.

IV. DISCUSSIONS

Although both our protocol and SLAZ2013 provide us ways to establish counterfactual communication, which is impossible with classical means, we should point out that they always fail in a secure scenario, such as quantum key distribution. The central problem is that no-cloning theorem is not included in their principles. Specifically, in both protocols, only orthogonal states, say, $|\phi_0\rangle$ and $|\phi_1\rangle$, are employed. Fortunately, it is not difficult to make them secure.

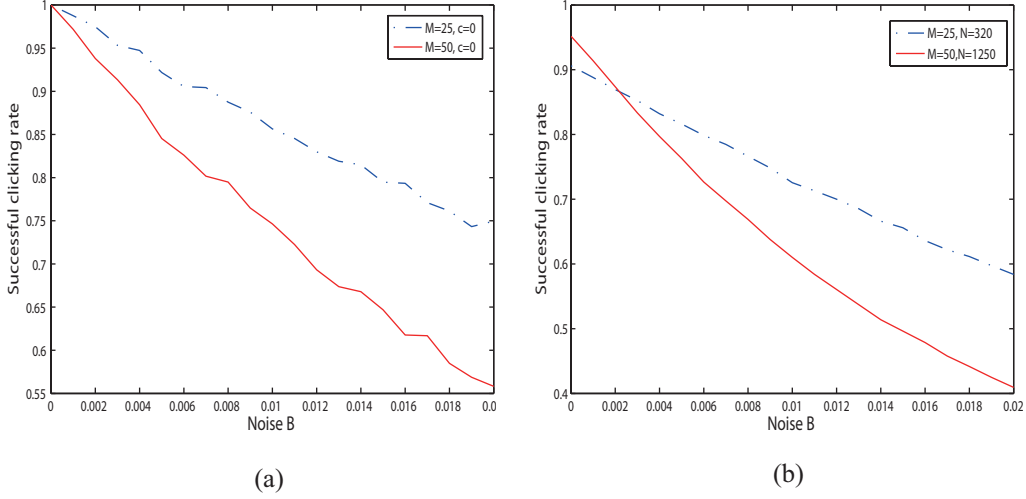


FIG. 4: Numerical estimating results. (a) Successful clicking rate of our protocol as a function of the noise rate B . Here, $c = 0$, corresponding to the worst case, is chosen as a better sample to make a comparison with SLAZ protocol. The solid(dash-dot) curve is plotted for $M = 25(50)$. (b) Successful clicking rate of SLAZ2013 protocol as a function of the noise rate B . The solid(dash-dot) curve is plotted for $M = 25(50)$, $N = 320(1250)$.

All one should do is to change the pure states into nonorthogonal mixed states, i.e., $\text{Tr}[\rho_0 \rho_1] \neq 0$. For this, Noh09 protocol acts as a good example. In doing so, our protocol immediately evolves to a quantum key distribution scheme. Here, we also highlight an open question that whether it is possible to explore unconditional security directly from quantum Zeno effect, thus leading to a new paradigm outperforming existed quantum key distribution schemes.

V. CONCLUSION

It is interesting that direct counterfactual quantum communication is achievable using quantum Zeno effect. However, the original scheme, i.e., SLAZ2013 protocol, has new problems when applying it in real channels. First, the efficiency is low, compared with conventional schemes. Second, it is too sensitive to noise. We find that those two flaws are resulted

from the nested structure, i.e., the inner cycles and outer cycles. In this paper, we succeeded in reducing the cycles by replacing the inner cycle with an iterative module, which is the core component of our new protocol. We have proved that perfect counterfactuality is achievable for our protocol, and showed that the a given level of performance can be reached with less cycles. Next, we further discussed the robustness of our protocol, and numerical estimating results showed that our scheme outperforms SLAZ2013 in the presence of noise. At last, we discussed how to bridge our protocol and quantum key distribution with no-cloning theorem, in order to broaden the view of direct counterfactual quantum communication.

VI. ACKNOWLEDGEMENTS

This work was supported by National Natural Science Foundation of China with the project number 61300203.

-
- [1] C. H. Bennett and S. J. Wiesner, Physical review letters **69**, 2881 (1992).
 - [2] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Physical Review Letters **76**, 4656 (1996).
 - [3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Physical Review Letters **70**, 1895 (1993).
 - [4] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Physical Review Letters **80**, 1121 (1998).
 - [5] T.-G. Noh, Phys. Rev. Lett. **103**, 230501 (2009).
 - [6] Y. Sun and Q. Y. Wen, Phys. Rev. A **82**, 052318 (2010).
 - [7] C. Bennett, G. Brassard, et al., in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984), p. 175.
 - [8] A. C. Elitzur and L. Vaidman, Found. Phys. **23**, 987 (1993).
 - [9] P. G. Kwiat et al., Phys. Rev. Lett. **83**, 4725 (1999).
 - [10] T. G. Noh and C. K. Hong, Quantum Semiclass. Opt. **10**, 637 (1998).
 - [11] Z. Sheng, W. Jian, and T. Chao-Jing, Communications in Theoretical Physics **59**, 27 (2013).
 - [12] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G. C. Guo, Phys. Rev. A **82**, 042335 (2010).
 - [13] Z. Sheng, W. Jian, and T. Chao-Jing, Chinese Physics B **21**, 060303 (2012).
 - [14] S. Zhang, J. Wnang, and C. J. Tang, EPL (Europhysics Letters) **98**, 30012 (2012).
 - [15] Y. Liu, L. Ju, X.-L. Liang, S.-B. Tang, G.-L. S. Tu, L. Zhou,

- C.-Z. Peng, K. Chen, T.-Y. Chen, Z.-B. Chen, et al., Physical review letters **109**, 030501 (2012).
- [16] G. Brida, A. Cavanna, I. P. Degiovanni, M. Genovese, and P. Traina, Laser Physics Letters **9**, 247 (2012).
- [17] H. Salih, Z.-H. Li, M. Al-Amri, and M. S. Zubairy, Physical review letters **110**, 170502 (2013).
- [18] H. Salih, Physical review A **90**, 012333 (2014).
- [19] A. Shenoy, R. Srikanth, and T. Srinivas, Physical Review A **89**, 052307 (2014).
- [20] H. A. Shenoy, R. Srikanth, and T. Srinivas, EPL (Europhysics Letters) **103**, 60008 (2013).
- [21] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, arXiv preprint arXiv:1404.6401 (2014).